UNITED STATES DISTRICT COURT

for the

Western District of Washington

FILED LODGED
RECEIVED
Apr 10 2023
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
BY DEPUTY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Five Namecheap Domains, controlled by Namecheap, Inc., located at 4600 East Washington St., Suite 305, Phoenix, AZ as further described in Attachment A-1

Case No. 3:23-mj-05131

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A-1, attached hereto and incorporated herein by reference.

located in the _____ District of Arizona , there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C §§1343, 1028A, 1956, and 1957.	Wire Fraud, Aggravated Identity Theft, Money Laundering, and Transactional Money Laundering.

The application is based on these facts:

✓ See Affidavit of Special Agent Heidi M. Hawkins, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Heidi M. Hawkins
Applicant's signature

Heidi M. Hawkins, FBI Special Agent
Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 04/10/2023

Theresa L. Fricke
Judge's signature

City and state: Tacoma, Washington

Theresa L. Fricke, United States Magistrate Judge
Printed name and title

AFFIDAVIT OF SPECIAL AGENT HEIDI M. HAWKINS

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Heidi M. Hawkins, being first duly sworn, depose and state as follows:

INTRODUCTION

A. Affiant Background

1. I am a Special Agent with the Federal Bureau of Investigation, currently assigned to the Seattle Field Office, and have been so employed since October 2019. My primary duties include investigating violations of federal law, including Title 18, United States Code, Sections 1343 (Wire Fraud), 1028A (Aggravated Identity Theft), 1956 (Money Laundering), 1957 (Transactional Money Laundering), and conspiracy to commit these offenses.

2. I attended and graduated from the Basic Field Training Course at the FBI Academy in Quantico, Virginia. At the FBI Academy, part of the training involved learning about the investigative value of the Internet, as well as ways the Internet can be criminally exploited to defraud others – especially in consideration of the relative ease with which it allows people to freely communicate with others. I am also personally familiar with the Internet and e-mail service providers, including Gmail and Yahoo email.

3. Based on my training and experience, I am familiar with the ways in which individuals involved in fraud schemes use shell e-mail accounts, the dark web, computers, cellular telephones, Internet Protocol addresses, fax numbers, shell companies, bank accounts, crypto-currency, synthetic identities, and counterfeit documents to facilitate fraudulent activity. I have learned that individuals perpetrating computer intrusions and identity theft-related bank fraud and wire fraud schemes employ a number of techniques, either alone or in combination, to further their illegal activities and to avoid detection by law enforcement. These techniques include: utilizing web-

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

based email accounts and other electronic messaging accounts to send, receive, store, and obtain personal identifying information, such as dates of birth and bank and credit card account numbers and related information; utilizing software programs or "spoofed" websites or email messages to dupe email recipients and others into downloading malicious software aimed at tracking and causing those individuals to unwittingly reveal or provide their personal identifying information or log-in credentials; using computers, servers, and other electronic devices to commit computer intrusions and to manufacture false identification documents and financial transaction cards; registering and using shell businesses to open multiple corporate bank accounts for the receiving and transferring of money; and employing a variety of other methods in furtherance of their schemes.

4. I am also familiar with the ways in which individuals involved in fraud schemes conceal, convert, transmit, and transport their illegal proceeds, including, but not limited to, the use of couriers and other third parties. I know that individuals involved in fraud schemes and money launderers hide bulk currency, financial instruments, documents relating to financial transactions, jewelry, automobiles, other items of value, and other proceeds, all of which constitute evidence of fraudulent activities. Additionally, such items constitute evidence of transactions establishing the generation, transfer, concealment, and expenditure of large sums of money made from engaging in fraudulent activities.

5. I know that individuals involved in fraud schemes often establish shell e-mail accounts and e-mail addresses in fictitious names and/or in the names of third parties in an effort to conceal their identities and illicit activities from law enforcement. I know that individuals involved in fraud often use virtual private network ("VPN") accounts and internet hosting services to conceal their true identities and geographical locations from law enforcement or other entities.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

B. Purpose of Affidavit

6. I am investigating a massive fraud on the Washington Employment Security Department (ESD) and other state workforce agencies (SWAs) responsible for administering pandemic unemployment claims. The fraud involves the theft of hundreds of billions of dollars that were intended to provide economic relief to American workers affected by the COVID-19 pandemic. The investigation has revealed that criminals submitted thousands of fraudulent unemployment claims to SWAs using the stolen personal identifying information of unwitting third persons. The fraudulent applications requested that the benefits be paid to bank account and payment cards controlled by persons known as "money mules," who withdrew and further dissipated the funds. The conduct under investigation violated numerous provisions of the United States criminal code, including Title 18, United States Code, Sections 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1028A (Aggravated Identity Theft), 1956 (Money Laundering), and 1957 (Transactional Money Laundering).

7. This affidavit is submitted in support of an application for a search warrant for information associated with:

a. the domain minderpower.com that is stored at premises controlled by Namecheap, Inc. (**TARGET ACCOUNT 1**);

b. the domain redfoxdna.com that is stored at premises controlled by Namecheap, Inc. (**TARGET ACCOUNT 2**);

c. the domain sensormargin.com that is stored at premises controlled by Namecheap, Inc. (**TARGET ACCOUNT 3**);

d. the domain unitedgsat.com that is stored at premises controlled by Namecheap, Inc. (**TARGET ACCOUNT 4**);

e. the domain quickjdna.com that is stored at premises controlled by Namecheap, Inc. (**TARGET ACCOUNT 5)**; and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. the email account js8979767@gmail.com that is stored at premises controlled by Google LLC (**TARGET ACCOUNT 6**).

8. Namecheap, Inc., dba Namecheap.com, is an electronic communications service based in Phoenix, Arizona. Google LLC is an electronic communications service based in Mountain View, California.

9. The information to be searched is described in the following paragraphs in Attachments A-1 and A-2. The requested warrant would require Namecheap and Google to disclose to law enforcement the material listed in Section I of Attachments B-1 and B-2, and would authorize law enforcement officers to search for, and seize, the material listed in Section II of Attachments B-1 and B-2.

10. The information set forth in this affidavit is not intended to detail each and every fact and circumstance of the investigation or all information known to me or the investigative participants. Rather, this affidavit is intended to present the facts relevant to the issue of whether probable cause exists to issue the requested search warrant.

11. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

STATEMENT OF PROBABLE CAUSE

A. Relevant Procedural History

12. On January 25, 2023, the Grand Jury in the Western District of Washington charged Fatiu Ismaila LAWAL and Sakiru Olanrewaju AMBALI with one count of Conspiracy to Commit Wire Fraud, in violation of Title 18 United States Code Section 1349; ten counts of Wire Fraud, in violation of Title 18 United States Code Sections 1343 and 2; and six counts of Aggravated Identity Theft, in violation of Title 18 United States Code Sections 1028A and 2.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

13. The indictment alleges that LAWAL, AMBALI, and their co-conspirators possessed and used the stolen personal identifying information of over 14,700 American workers and taxpayers to fraudulently obtain United States government funds, including COVID-19 pandemic unemployment benefits, pandemic assistance for small businesses, and federal tax refunds. Specifically, LAWAL and AMBALI, both Nigerian nationals and Canadian residents, and their co-conspirators used these stolen identities to submit over 1,700 claims for COVID-19 pandemic-related unemployment benefits to over 25 SWAs and over 2,300 fraudulent tax returns to the Internal Revenue Service. They also used the stolen identities to seek pandemic assistance from the United States Small Business Administration. In doing so, LAWAL and AMBALI, together and with their co-conspirators, caused and attempted to cause, state and federal agencies to pay out approximately $25 in government funds. They successfully obtained over $2.4 million, primarily from pandemic unemployment benefits.

B. The CARES Act

14. Based on publicly-available information, I know that on March 27, 2020, the United States enacted into law the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The CARES Act authorized approximately $2 trillion in aid to American workers, families, and businesses to mitigate the economic consequences of the COVID-19 pandemic. The CARES Act funded and authorized each state to administer new unemployment benefits. These benefits include (1) Federal Pandemic Unemployment Compensation (FPUC), which provides an additional benefit of $600 per week per unemployed worker; (2) Pandemic Unemployment Assistance (PUA), which extends benefits to self-employed persons, independent contractors, and others; and (3) Pandemic Emergency Unemployment Assistance (PEUC), which extends benefits for an additional 13 weeks after regular unemployment benefits are exhausted. All of these programs will be referenced herein as "CARES Act benefits." The CARES Act allows an unemployed

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

worker to obtain back benefits retroactive to the date on which the applicant was affected by COVID 19, which, under program rules, may be as early as February 2, 2020.

C. Overview of Investigation

15. Beginning on around April 20, 2020, law enforcement officials began receiving complaints from employers about potentially fraudulent unemployment claims. The employers reported that they had received notices from ESD indicating that persons still under their employ had filed unemployment claims. For example, on or about April 20, 2020, the Seattle Fire Department (SFD) notified the U.S. Attorney's Office for the Western District of Washington that claims had been filed in the names of multiple firefighters who were actively employed by SFD. SFD reported that it had interviewed the firefighters, who had denied any involvement in the claims. Other employers, including Microsoft Corporation, the City of Bellingham, Zulily, and Seattle Yacht Club submitted similar complaints.

16. Roughly around that same time, numerous other agencies, including the Federal Bureau of Investigation, the Social Security Administration Office of Inspector General, the United States Secret Service, the Department of Labor Office of the Inspector General (DOL-OIG), the United States Postal Inspection Service, and Internal Revenue Service Criminal Investigation, joined the investigation. Agents from these agencies, including myself, have reviewed voluminous financial records and databases reflecting the fraudulent transactions and have conducted dozens of interviews.

17. The investigation has developed evidence that hundreds of millions worth of fraudulent claims were filed with ESD using the stolen personal identifying information of Washington residents. The FBI investigation has determined that many of the fraudulent claims were filed using internet protocol (IP) addresses that resolve to Nigeria. While the actual amount of loss is unknown, the Washington State Auditor has issued a report finding that ESD paid out at least $642,954,417 in fraudulent imposter claims, of which $369,789,082 has been recovered. Numerous other SWAs were

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

victimized in the same manner, often by persons using the same email addresses or IP addresses as the persons who defrauded ESD.

18. The FBI's review of ESD records and other financial records indicates that the fraud proceeds were paid out to financial accounts controlled by "money mules," that is, persons under the control of the criminals who orchestrated the fraud. The money mules withdrew the fraud proceeds from their account and dissipated the money in accordance with instructions given to them.

D. Role of Gmail Accounts in the Fraud

19. One source of data in the investigation is a database produced by ESD containing claims information that ESD believed to be fraudulent. I have used the database to generate numerous leads, and my investigative activities have confirmed that, for those leads I have investigated, the claims are indeed fraudulent. The database includes email addresses used to submit each fraudulent claim, including over 30,000 Goggle-hosted email accounts. Another source of data in the investigation is a database maintained by the DOL-OIG, which includes claims data from all 54 SWAs in the country responsible for distributing CARES Act benefits. I have used the database to generate numerous leads, and my investigative activities have confirmed that, for those leads I have investigated, the claims are indeed fraudulent. The database includes email addresses used to submit each fraudulent claim, the amount of benefits paid, and other relevant claims data.

20. For many of the Google email accounts in the ESD database, perpetrators took advantage of a particular feature of Google email accounts that allowed them to submit multiple fraudulent claims from a single Google email account, without ESD detecting that a single email address was being used repeatedly. Specifically, in routing emails to an email box, Google disregards periods in the email address, meaning that the email address "john.doe@gmail.com" and "johndoe@gmail.com" will resolve to the same Google email account, even though ESD identifies them as two different accounts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Two email addresses like these that are distinguished only by periods are known as "Google variants" or "dot variants." I know from my training and experience that criminals sometimes take advantage of this feature to make it appear that emails are originating from multiple accounts, when in fact they originate from the same account. This reduces the number of email accounts that a criminal must open and monitor while perpetrating a fraud, while avoiding fraud alerts that may be triggered when multiple claims originate from the same account.

E. Gmail Accounts and LAWAL.

21. **gamework393@gmail.com.** Investigators analyzed ESD's database to identify Gmail accounts that were used to submit multiple claims using the Google dot variant method discussed above. Among these accounts was an account with the address gamework393@gmail.com.

22. According to DOL-OIG's records, beginning on or about May 6, 2020, dot variants of gamework393@gmail.com (g.a.mew.o.r.k.3.93@gmail.com, g.a.mewor.k.3.9.3@gmail.com, and ga.mew.o.r.k.39.3@gmail.com.) were used to submit approximately 27 claims to ESD and more than 160 claims to 11 other SWAs to obtain benefits exceeding $795,000.

23. On August 19, 2021, Judge David W. Christel authorized a search warrant for the gamework393@gmail.com account hosted by Google. The contents of the account yielded evidence that LAWAL is the true user of the account.

24. For example, the Google Drive for gamework393@gmail.com contained a Nigerian bank statement in the name of LAWAL's son, M.L., whose identity was verified through U.S. government visa records for LAWAL and M.L. Specifically, M.L. applied for a U.S. visitor visa in 2018, and LAWAL is listed as his father. The email listed on the application is limapasco@yahoo.com, which federal investigators also linked to LAWAL and gamework393@gmail.com, in part, through a common IP address (206.176.145.184), which was used to access both accounts on November 26, 2020 and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

November 27, 2020. On February 28, 2022, Judge Christel authorized a search warrant for limapasco@yahoo.com. The contents of the Yahoo account referenced the family's U.S. visa applications and M.L.'s application and confirmation were attached to an email.

25. The Google Drive bank statement in M.L.'s name shows that between March 1, 2020 and July 22, 2020, the "Smart Kids Save" account balance at a Nigerian bank grew from the equivalent of approximately $8.00 USD to $70,000 USD, with the statement remarks showing that nearly all of the deposits originated from an account belonging to "LAWAL, FATIU ISMAILA." Based on DOL-OIG records, during that same time period, gamework393@gmail.com was used to file over 100 pandemic unemployment claims, resulting in benefit payments of over $80,000 USD.

26. The gamework393@gmail.com account's internet search history on August 31, 2020, showed that the user looked up a FedEx tracking number, 811321800534. FedEx records showed that a package was shipped from Lagos, Nigeria to "LAWAL FATIU ISMAILA" at an address in Scarborough, Ontario, Canada. An email found in limapasco@yahoo.com and dated December 14, 2020, had a subject line "ADDRESSES LAWAL," and a message that stated, "10 YEARS BACK ADDRESSES I LIVED" and listed six addresses beginning in Lagos, Nigeria in September 2008 and ending in Ontario, Canada. Among the addresses was the Scarborough address, where LAWAL lived from March 30, 2020, until November 6, 2020.

27. The limapasco@yahoo.com account contained additional evidence that LAWAL is the true user of gamework393@gmail.com. For example, the subscriber name for the account is an inversion of LAWAL's middle and first names, "Ismaila Fatiu." The recovery email for the Yahoo account is js755641@gmail.com, which is linked by common cookies with gamework393@gmail.com and was accessed using a common IP address (see paragraphs 29-30). The Yahoo account also contained copies of LAWAL's birth certificate, Canadian immigration documents, and various bank statements.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

28. The evidence described above gives me a reasonable belief that LAWAL controls gamework393@gmail.com.

29. **Linked Accounts.** Google records also show that gamework393@gmail.com shares cookies with multiple Gmail accounts, including the following four: limapasco@gmail.com, bankupdates2014@gmail.com, js755641@gmail.com, and js755642@gmail.com (Linked Accounts). A cookie or "cookie overlap" consists of small files stored by Google monitoring the user's activity while logged into the account. Cookie overlap indicates that the accounts were accessed from the same web browser or computer. This evidence, in turn, suggests that both accounts were accessed by a common user. Based on my training and experience, accounts linked by cookies assist with determining who controls the email account by identifying other emails and individuals relevant to the investigation. Accordingly, LAWAL likely also controls the Linked Accounts.

30. On March 25, 2022, this Court authorized a search warrant for six Gmail accounts, including the four Linked Accounts. Records for the Linked Accounts further confirmed that LAWAL controls the Linked Accounts. For example, Google and Yahoo records also show that a common IP address (2607:fea8:3220:c200:a17d:1faa:8f32:aed9) was used to log into limapasco@yahoo.com, limapasco@gmail.com, js755641@gmail.com, and bankupdates2014@gmail.com on May 18, 2021. And on August 9, 2021, within seven minutes, a common IP address (2607:fea8:3220:6f00:dde:8a12:cc24:ac2) was used to log into js755641@gmail.com and gamework393@gmail.com. And again, on October 23, 2021, within an approximate 10-minute time frame, js755642@gmail.com, js755641@gmail.com, and limapasco@gmail.com were all accessed using a common IP address (2607:9880:2ce0:11:f5f5:9167:d8b4:4f74). All three of these overlapping IP addresses resolved in Canada where LAWAL was residing at the time of the account access. Based on my training and experience, contemporaneous use of the same IP address to log

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

into multiple accounts indicates that the accounts were accessed from the same device and suggests a common user.

31. The inbox of bankupdates2014@gmail.com also contained additional evidence that LAWAL controls the Linked Accounts, including emails addressed to "Fatiu Ismaila Lawal" and "Lima" and "limadon." The account contents also included emails sent to other Linked Accounts, such as js755641@gmail.com, that contained large volumes of personal identifying information of American residents.

32. The js755641@gmail.com account also contained connections to LAWAL and fraud. The contents of the js755641 Google Drive included step-by-step tutorials of how to file unemployment claims for various SWAs and images of debit cards issued by SWAs to disburse benefits. The js755641 Google Drive also contained photos of LAWAL, images of his birth certificate, and documents related to LAWAL's Nigerian and Canadian driver's license.

33. The evidence described above gives me a reasonable belief that LAWAL controls the Linked Accounts.

34. **vac22334@gmail.com.** According to DOL-OIG's records, beginning on or about May 4, 2020, dot variants of vac2234@gmail.com were used to submit approximately 30 pandemic unemployment claims to various SWAs nationwide (with about half of the claims submitted to ESD), resulting in the payment of benefits totaling approximately $109,000. On or about May 4, 2020, a claim was submitted to ESD using the identity of R.R. and vac.2.2334@gmail. The address for this claim was an address in Concrete, Washington. In an interview with federal investigators, R.R. confirmed that she neither filed an unemployment claim on or about May 4, 2020, nor did she authorize anyone to do so on her behalf.

35. According to the internet search history of gamework393@gmail.com, on or about May 10, 2020, LAWAL searched for R.R.'s address in Concrete, Washington. Additionally, attached to an email in the gamework393@gmail.com account dated April

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

26, 2020, is a file named "GOOD CREDIT.txt." Listed in that file are dozens of entries with the personal identifying information of Americans including R.R. The entry for R.R. lists her Social Security number, date of birth, and address.

36. Records from Metropolitan Commercial Bank further show that a common device was used to access MOVOCash accounts opened using dot variants of gamework393@gmail.com and vac22334@gmail.com. MOVOCash is a prepaid card program that distributes its "cards" via mobile applications, thereby the funds are accessible from any electronic device. MOVOCash records show that an account ending in -3167 was opened on about June 14, 2020, using a dot variant of vac22334@gmail.com. The records show that New York's SWA attempted to deposit $1104 on June 18, 2020, but the deposit was declined. Bank records show that MOVOCash account ending in -0752 was opened on June 15, 2020, using a dot variant of gamework393@gmail.com. Between June 18, 2020, and June 24, 2020, New York's SWA made multiple deposits into the account, but a portion was returned due to suspected fraud. The records further show that on June 20, 2020, the dot variant vac22334@gmail.com MOVOCash account was accessed through a device with the ID 86ca4402-d574-40c3-a54f-a0bc61d4de6f. The same device accessed the dot variant gamework393@gmail.com MOVOCash account twice the next day.

37. The search warrant this court authorized on March 25, 2022 for six Gmail accounts also included vac22334@gmail.com. The contacts for vac22334@gmail.com included an entry for "limapasco" with two phone numbers: one Nigerian number ending in -8021 and one Canadian number ending in -5650. The contents of the vac22334@gmail.com inbox included an email with the subject "LAWAL ADDRESSES," and it had 19 file attachments, all of which were completed unemployment benefit applications for California's SWA, the Employment Development Department (EDD). Each attachment followed the same naming convention that ends with "LAWAL" and a number as a suffix. For example, the application for the identity

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of S.F. is saved as "EDD (1) [REDACTED LAST NAME] [REDACTED FIRST NAME]…LAWAL 003."

38. The evidence described above gives me a reasonable belief that the user of vac22334@gmail.com is a co-conspirator in a common fraudulent scheme with LAWAL.

E. TARGET ACCOUNTS 1 through 5—Namecheap.

39. **Connections to LAWAL and Co-Conspirator.** The email contents of gamework393@gmail.com and vac22334@gmail.com included emails from internet domain registrar Namecheap, indicating that each account also had domains registered with Namecheap.

40. For example, the vac22334@gmail.com inbox contained approximately nine emails from Namecheap, including one about tips for using its Private Email service. A Namecheap order summary dated March 12, 2022, showed that the account registered **TARGET ACCOUNT 5** with "Pro Email" service and three mailboxes.

41. The inbox for gamework393@gmail.com contained approximately 100 emails from Namecheap, including notices and confirmations about renewing domain names and automatic payments for subscription services. The internet history for the gamework393@gmail.com account also showed that on January 2, 2021, LAWAL searched for "how to buy private email on namecheap" and visited a website about how to order Namecheap Private Email service.

42. Namecheap records confirm that an account registered to gamework393@gmail.com was opened on December 18, 2020, with the user ID "limapasco," using the name J.B. and an address in Hyattsville, Maryland. J.B.'s name and the Hyattsville, Maryland address were also found in a message that gamework393@gmail sent on April 16, 2021, amongst a long list of other web logins, passwords, links to state workforce agency application websites, and financial account numbers. The phone number associated with the gamework393@gmail.com Namecheap account is a Dallas phone number ending in -3906. This number is also associated with a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Bank of America account that received approximately $20,000 in California unemployment benefits and was opened using a dot variant of gamework393@gmail.com. The Namecheap records show that the account has Private Email subscriptions for four domain names, **TARGET ACCOUNTS 1 through 4**.

43. During the course of my investigation, I learned that Namecheap's Private Email service allows the domain owner to access emails sent to any unique email address within that domain.

44. **Used for Fraud.** Namecheap records show that **TARGET ACCOUNT 1** (minderpower.com) was created on June 7, 2021 and remains active. DOL-OIG records show that, between June 15, 2021 and December 28, 2021, emails using this domain (e.g. berry9360@minderpower.com, holleyrf5@minderpower.com) submitted over 150 fraudulent unemployment claims to various SWAs including Washington, Maryland, and Pennsylvania. Internal Revenue Service (IRS) records also show that email addresses associated with **TARGET ACCOUNT 1** filed approximately 375 tax returns for tax years 2020 and 2021, seeking over $650,000 in tax refunds. Small Business Administration (SBA) records show at least four Economic Injury Disaster Loans (EIDL) associated with emails (e.g. rm@minderpower.com, dearcionette54@minderpower.com) using **TARGET ACCOUNT 1**. All loans were flagged as fraudulent and not funded.

45. Namecheap records also show that **TARGET ACCOUNT 2** (redfoxdna.com) was created on March 25, 2021 and remains active. DOL-OIG records show that, between March 21, 2021 and June 26, 2021, emails using this domain (e.g. ddd13ddd@redfoxdna.com, drsock@redfoxdna.com) submitted over 15 fraudulent unemployment claims to various SWAs including New York, Maryland, and Pennsylvania. IRS records also show that email addresses associated with **TARGET ACCOUNT 2** filed over 570 tax returns for the 2021 tax year. SBA records indicate that email addresses associated with **TARGET ACCOUNT 2** were used to file at least three Paycheck Protection Program (PPP) loan applications. SBA denied the applications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

46. Namecheap records show that **TARGET ACCOUNT 3** (sensormargin.com) was created on December 18, 2020, and remains active. DOL-OIG records show that, between December 18, 2020 and June 6, 2022, emails using this domain (e.g. 000@sensormargin.com, nnnn@sensormargin.com) submitted 474 fraudulent unemployment claims, to SWAs in various states, including Washington, California, Massachusetts, and New York. IRS records also show that email addresses associated with **TARGET ACCOUNT 3** filed over 1100 tax returns for the tax years 2020 and 2021, seeking refunds of over $1.9 million and resulting in the payment of at least $29,000 in refunds.

47. SBA records show at least 10 EIDL applications associated with emails using **TARGET ACCOUNT 3**. One of the applications was funded on or about November 7, 2021, using the email address jamesm@sensormargin.com. SBA emailed the loan applicant on October 19, 2021, at approximately 7:50 p.m., using email jamesm@sensormargin.com. Shortly later, at approximately 8:13 p.m., a response was received from email address admin@sensormargin.com. This suggests the same person is in control of jamesm@sensormargin.com and admin@sensormargin.com.

48. Namecheap records show that **TARGET ACCOUNT 4** (unitedgsat.com) was created on April 22, 2021 and remains active. DOL-OIG records show that, between April 23, 2021 and June 10, 2022, emails using this domain (e.g. robbchris@unitedgsat.com, jameshyv@unitedgsat.com) submitted over 160 fraudulent unemployment claims to various SWAs including California, New York, Maryland, and Pennsylvania. IRS records also show that email addresses associated with **TARGET ACCOUNT 4** filed over 580 tax returns for the 2021 tax year, seeking refunds of approximately $3 million. SBA records indicate that six EIDL applications and one PPP loan application was submitted by emails using **TARGET ACCOUNT 4**.

49. Open-source research revealed that **TARGET ACCOUNT 5** (quickjdna.com) is registered with Namecheap through March 13, 2024. IRS records

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

show that email addresses associated with **TARGET ACCOUNT 5** filed 65 tax returns for the 2021 tax year.

50. In summary, based on the evidence described above and my training and experience, I have a reasonable basis to believe that **TARGET ACCOUNTS 1 through 5** contain evidence of fraud, conspiracy, and money laundering, and that its true user of **TARGET ACCOUNTS 1 through 4** is LAWAL and the true user of **TARGET ACCOUNT 5** is LAWAL's co-conspirator in a common scheme to defraud the United States government.

E. TARGET ACCOUNT 6—Google.

51. **Connections to LAWAL.** Google records show that the **TARGET ACCOUNT 6** (js8979767@gmail.com) was created on May 26, 2016 and remains active. Google records also indicate that the **TARGET ACCOUNT 6** shares cookies with gamework393@gmail.com and LAWAL's Linked Accounts. **TARGET ACCOUNT 6**'s recovery email address is gamework393@gmail.com. A recovery email address assists an account user to access its account by receiving security notifications and messages that allow the user to regain access to its account. Based on my training and experience, the user of an account and the user of the account's recovery email are a common user. In this case, that common user is LAWAL.

52. The **TARGET ACCOUNT 6** also appears in a document saved in gamework393's Google Drive that lists dozens of logins and passwords for websites and accounts. The entries in the document are generally consistent in format: first listing a website or application name, followed by a telephone number, an email address or username, and ending with a password. One entry provides login information for a Google Voice telephone number (which is also used for the Namecheap account associated with gamework393@gmail.com):

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

MY GOOGLE VOICE
[REDACTED] -3906
Successful
John Smith
Js8979767@gmail.com **[TARGET ACCOUNT 6]**
[REDACTED PASSWORD]

Additionally, the **TARGET ACCOUNT 6** has multiple connections to one of LAWAL's Linked Accounts, js744641@gmail.com. According to Google records, both accounts use the subscriber name John Smith. Based on my training and experience, fraudsters often use alias subscriber names for email accounts used for criminal activity. In addition to sharing cookies, both accounts were accessed on August 20, 2021, using a common IP address: 2607:9880:2ce0:11:e5b9:e8f2:29cc:dac9, which resolves to an internet service provider in Canada where LAWAL resided in 2021. **TARGET ACCOUNT 6** is also the recovery email address for js755641@gmail.com.

53. **Used for Fraud.** DOL-OIG records show that a dot variant of the **TARGET ACCOUNT 6** submitted at least one fraudulent claim in the identity of F.J., on or around January 7, 2021, to the SWA for the District of Columbia. The claim was flagged as suspicious and not paid. Google records also revealed that the gamework393@gmail.com Namecheap phone number ending in -3906 was used to access the **TARGET ACCOUNT 6** and is associated with its Google Pay billing information. The same -3906 phone number was used to file at least 25 fraudulent unemployment applications associated with gamework393@gmail.com and two Linked Accounts, js755642@gmail.com and bankupdates2014@gmail.com.

54. In summary, based on the evidence described above and my training and experience, I have a reasonable basis to believe that LAWAL is the true user for **TARGET ACCOUNT 6**, and the **TARGET ACCOUNT 6** contains evidence of fraud, conspiracy, and money laundering.

BACKGROUND REGARDING PROVIDERS' SERVICES

55. Information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time.

56. Information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

57. Stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

58. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation, because the information can be used to identify the account's user or users.

59. In general, an email that is sent to a subscriber is stored in the subscriber's "mail box" on the email provider's servers until the subscriber deletes the email. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to the provider's servers, and then transmitted to its end destination. The email provider often maintains a copy of received and sent emails. Unless the sender specifically deletes an email from the email provider's server, the email can remain on the system indefinitely. Even if the subscriber deletes the email, it may continue to be available on the email provider's servers for some period of time.

60. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by the email provider but may not include all of these categories of data.

Google's Services

61. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the general public. Google provides subscribers email and chat account at the domain name "@gmail.com."

62. Subscribers obtain an account by registering with Google. When doing so, Google asks the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

63. Google typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. As with subscriber records, IP address information can help to identify which computers or other devices were used to access the email account, which in turn can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

64. In addition to email and chat, Google offers subscribers numerous other services including, (i) Location History, which saves information about the physical locations of devices logged into a Google account; and (ii) Web & Activity, which saves information about Google web searches and browsing activity conducted by a user logged into a particular Google account.

Namecheap's Services

65. In my training and experience, I have learned that Namecheap provides a variety of on-line services, including domain name registration, web hosting, as well as email access. Namecheap allows subscribers to register and maintain domains for use on the Internet (e.g., sensormargin.com) and to further create and use email accounts under those such domain names (e.g., admin@sensormargin.com), including **TARGET ACCOUNTS 1 through 5** discussed above and listed in Attachment A-1. Namecheap's Private Email service is a fee-based email interface that provides email, calendar and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contacts, tasks management and document storage services. There are three Private email service subscriptions: Starter, Pro and Ultimate. Each subscription provides the user with one to five mailboxes and additional features depending on the subscription. One feature available in all three services is the catch-all (wildcard) email address forwarding option.

66. The wildcard email address is the account's catch-all address. This means that any email sent to the subscriber's domain that is not yet set up to be an email account will be sent to the wildcard address for the account. The user must set up the catch-all forwarding option within the accounts settings by selecting the domain (i.e., @sensormargin) and then choosing the option to add catch-all. Once selected, all emails sent to the domain (wildcard email address) will be sent to its inbox making it easier for the user to manage. For instance, emails 123@sensormargin.com, ABC@sensormargin.com, and 45DE@sensormargin.com would all be routed to the same inbox.

67. Of note, the user cannot send outgoing emails using the catch-all emails. The mailbox can only receive catch-all emails. The user can only send emails from the primary mailbox. For example, as described above in paragraph 47, SBA emailed the EIDL applicant jamesm@sensormargin.com about a loan application. SBA received a response from admin@sensormargin.com, not jamesm@sensormargin.com, indicating that the admin@sensormargin.com is the primary mailbox for the account.

68. Subscribers obtain an account by registering with Namecheap. When doing so, e-mail providers like Namecheap ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identify the account's user or users, and to help establish who has dominion and control over the account.

INFORMAITON TO BE SEARCHED AND THINGS TO BE SEIZED

69. This Application seeks a warrant to search all responsive records and information under the control of Google and Namecheap, providers subject to the jurisdiction of this court, regardless of where Google and Namecheap has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's or Namecheap's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

70. This warrant will be executed under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google and Namecheap to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachment B-1 and B-2.

CONCLUSION

71. Based on the foregoing, I believe there is probable cause to believe that evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States Code, Sections 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1956 (Money Laundering), 1957 (Money Laundering), and 1028A (Aggravated Identity Theft) will be found **TARGET ACCOUNTS 1 through 6**, as more fully described in Attachments A-1 and A-2 of this Affidavit. I therefore request that the Court issue

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

warrants authorizing a search of **TARGET ACCOUNTS 1 through 6**, for the items more fully described in Attachment B-1 and B-2, incorporated herein by reference, and the seizure of any such items found therein.

72. Because the warrant will be served on Google and Namecheap, which will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Heidi M. Hawkins
HEIDI M. HAWKINS
Special Agent
Federal Bureau of Investigation

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit on this 10th day of April, 2023.

Theresa L. Fricke
THERESA L. FRICKE
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Property to Be Searched

This warrant applies to the electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following domains (collectively, **the Domains**):

- minderpower.com;
- redfoxdna.com;
- sensormargin.com;
- unitedgsat.com; and
- quickjdna.com,

including all Private Email Subscription email content of the Domains and all other subscriber and log records associated with the domains, which are located at premises owned, maintained, controlled or operated by **Namecheap, Inc., dba Namecheap.com**, an electronic communications service and/or remote computer service provider located at 4600 East Washington Street, Suite 305, Phoenix, AZ 85034.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Namecheap, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the Domains identified in Attachment A-1:

(a) The contents of all e-mails associated with the domains from **December 18, 2020, to the present**, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

(b) All saved "drafts" of unsent or communications;

(c) All location data;

(d) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

(e) The types of service utilized by the user;

(f) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

data, pictures, and files;

(g) All information about connections between the account and third-party websites and applications;

(h) All records pertaining to communications between Namecheap and any person regarding the account, including contacts with support services, and all records of actions taken, including suspensions of the account;

(i) All complaints and records relating to any adverse action taken on the account, including an account suspension for violations of terms of service, whether temporary or permanent, the details surrounding that adverse action, and any communications related thereto.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

Upon receipt of the information described in Section I, the government shall review the production and may seize the following material:

The following information that constitutes evidence and instrumentalities of violations of Title 18 United States Code, Sections 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1956 (Money Laundering), 1957 (Money Laundering), and/or 1028A (Aggravated Identity Theft) for the Domains:

a. Material referring or relating to any claims for benefits from the United States government or the government of any U.S. state;

b. Material referring or relating to any U.S. tax return or other U.S. tax filings;

c. Material containing personal identifying information or account access information of any person;

d. Material referring or relating to any financial transactions, accounts, and/or purchases;

e. Material that serves to identify any person who uses or accesses or who exercises in any way any dominion or control over the Domains;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Material evidencing the times and methods by which the Domains was accessed;

g. Material that serves to identify any persons connected to any person who accesses or who exercises in any way any dominion or control over the Domains; and

h. Material evidencing the user's state of mind as it relates to the crimes under investigation;

i. Material that serves to identify any other accounts related to the Domains; including accounts that share common recovery information or that are linked by cookies or in any other way;

h. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over the account as well as records or information that may reveal the true identities of these individuals;

i. Log records, including IP address captures, associated with the account;

j. Subscriber records associated with the account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Namecheap in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

k. Records of communications between Namecheap and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications;

l. Android or Apple identification number, MEID, and cellular telephone number; and

m. Information identifying accounts that are linked or associated with the account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Property to Be Searched

This warrant applies to the electronically stored data, information and communications contained in, related to, and associated with, including all preserved data, the following account **Js8979767@gmail.com** (**the Account**), as well as all other subscriber and log records associated with the Account, which is located at premises owned, maintained, controlled or operated by Google LLC, an email and service provider that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for the Account identified in Attachment A-2:

j. The contents of all emails associated with the Account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each emails, the date and time at which each email was sent, and the size and length of each email;

k. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

l. All records or other information stored by any individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

m. any Google Chat/Messenger information and/or records, including any contact or friend list, time, date, and IP address logs for Chat and Messenger use, and any archived web messenger communications stored on servers;

n. any Google Search Console content from inception to the present;

o. any Google Web & Activity content from inception to the present;

p. any Google Chrome Sync content from inception to the present;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

q. any Google Location History content from inception to the present;

r. any account history, including any records of communications between Google and any other person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service;

s. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

Upon receipt of the information described in Section I, the government shall review the production and may seize the following material:

The following information that constitutes evidence and instrumentalities of violations of Title 18 United States Code, Sections 1343 (Wire Fraud), 1349 (Conspiracy to Commit Wire Fraud), 1956 (Money Laundering), 1957 (Money Laundering), and/or 1028A (Aggravated Identity Theft) for Account:

t. Material referring or relating to any claims for benefits from the United States government or the government of any U.S. state;

u. Material referring or relating to any U.S. tax return or other U.S. tax filings;

v. Material containing personal identifying information or account access information of any person;

w. Material referring or relating to any financial transactions, accounts, and/or purchases;

x. Material that serves to identify any person who uses or accesses or who exercises in any way any dominion or control over the Account;

y. Material evidencing the times and methods by which Account was accessed;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

z. Material that serves to identify any persons connected to any person who accesses or who exercises in any way any dominion or control over the Account; and

aa. Material evidencing the user's state of mind as it relates to the crimes under investigation;

bb. Material that serves to identify any other accounts related to the Account; including accounts that share common recovery information or that are linked by cookies or in any other way;

n. Content that may identify any alias names, online user names, "handles" and/or "nics" of those who exercise in any way any dominion or control over the account as well as records or information that may reveal the true identities of these individuals;

o. Log records, including IP address captures, associated with the account;

p. Subscriber records associated with the account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, Including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP addresses, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

q. Records of communications between Google and any person purporting to be the account holder about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications;

r. Android or Apple identification number, MEID, and cellular telephone number; and

s. Information identifying accounts that are linked or associated with the account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970